(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平7－134547

(43)公開日　平成７年(1995)５月23日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０９Ｃ	1/00		9364－5L		
Ｈ０４Ｌ	9/06				
	9/14				
				Ｈ０４Ｌ　9/ 02　Ｚ	

審査請求　未請求　請求項の数20　ＯＬ　（全 13 頁）

(21)出願番号　特願平5－281295

(22)出願日　平成５年(1993)11月10日

(71)出願人　000005810
日立マクセル株式会社
大阪府茨木市丑寅１丁目１番88号

(72)発明者　中村　▲昂▼
大阪府茨木市丑寅一丁目１番88号　日立マクセル株式会社内

(74)代理人　弁理士　武　顕次郎

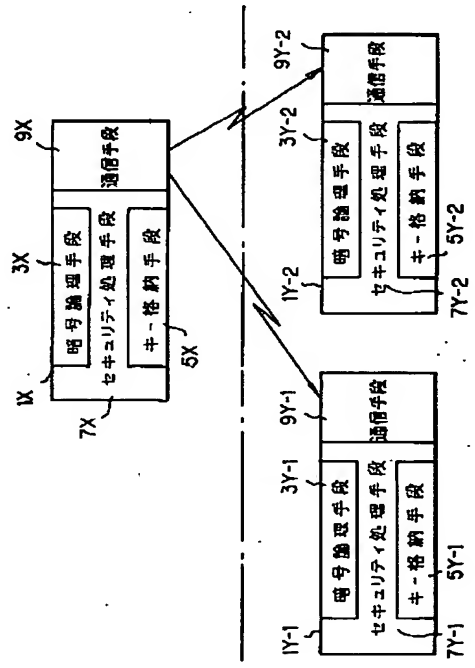
(54)【発明の名称】　情報の受渡しシステムならびにそれに用いる暗号処理装置

(57)【要約】

【目的】　機密性の高い情報の受渡しシステムを提供する。

【構成】　少なくとも第１の端末装置１Ｘと第２の端末装置１Ｙとの間で情報の受渡しを行う情報の受渡しシステムにおいて、次の処理工程を含んでいることを特徴とする。前記第１の端末装置１Ｘで、情報の利用者間で共通する共通キーを生成し、その第１の端末装置１Ｘにおいて、情報利用者毎に個別に設定された個別キーで前記共通キーを暗号化して個別のワークキーを生成し、そのワークキーを前記第２の端末装置１Ｙに渡し、第２の端末装置１Ｙが有している個別キーを用いて、前述の渡されたワークキーを復号化して共通キーを生成し、渡す情報を前記共通キーで暗号化して暗号化情報を生成し、第１の端末装置１Ｘまたは第２の端末装置１Ｙから、他方の端末装置へ暗号化された情報を渡し、その渡された暗号化情報を共通キーを用いて元の情報に復号化する。

【図１】



1

【特許請求の範囲】

【請求項１】　少なくとも第１の端末装置と第２の端末装置との間で情報の受渡しを行う情報の受渡しシステムにおいて、次の処理工程を含んでいることを特徴とする情報の受渡しシステム。前記第１の端末装置で、情報の利用者間で共通する共通キーを生成し、

その第１の端末装置において、情報利用者毎に個別に設定された個別キーで前記共通キーを暗号化して個別のワークキーを生成し、

そのワークキーを前記第２の端末装置に渡し、

第２の端末装置が有している個別キーを用いて、前述の渡されたワークキーを復号化して共通キーを生成し、

渡す情報を前記共通キーで暗号化して暗号化情報を生成し、

第１の端末装置または第２の端末装置から、他方の端末装置へ暗号化された情報を渡し、

その渡された暗号化情報を共通キーを用いて元の情報に復号化する。

【請求項２】　少なくとも第１の端末装置と第２の端末装置と第３の端末装置の間で情報の受渡しを行う情報の受渡しシステムにおいて、次の処理工程を含んでいることを特徴とする情報の受渡しシステム。前記第１の端末装置で、情報の利用者間で共通する共通キーを生成し、

その第１の端末装置において、情報利用者毎に個別に設定された個別キーで前記共通キーを暗号化して個別のワークキーを生成し、

そのワークキーを前記第２の端末装置ならびに第３の端末装置にそれぞれ渡し、

第２の端末装置ならびに第３の端末装置が有している個別キーを用いて、前述の渡されたワークキーを復号化して共通キーを生成し、

渡す情報を前記共通キーで暗号化して暗号化情報を生成し、

第１の端末装置、第２の端末装置、第３の端末装置の間で暗号化された情報を渡し、

その受渡たされた暗号化情報を共通キーを用いて元の情報に復号化する。

【請求項３】　請求項１または２記載において、前記個別キーを前記第１の端末装置で生成して、各個別キーを他の端末装置に渡すように構成されていることを特徴とする情報の受渡しシステム。

【請求項４】　請求項３記載において、前記第１の端末装置から第２の端末装置ならびに第３の端末装置への個別キーとワークキーの受渡しが別ルートになっていることを特徴とする情報の受渡しシステム。

【請求項５】　請求項３記載において、前記個別キーを先に渡し、その後にワークキーまたは（ならびに）暗号化情報を渡すように構成されていることを特徴とする情報の受渡しシステム。

【請求項６】　請求項１または２記載において、前記ワークキーと暗号化情報が同時に渡されるように構成されていることを特徴とする情報の受渡しシステム。

2

【請求項７】　請求項１または２記載において、前記ワークキーと暗号化情報が時間的にずらして渡されるように構成されていることを特徴とする情報の受渡しシステム。

【請求項８】　請求項１または２記載において、前記個別キーまたは（ならびに）共通キーが変更可能であることを特徴とする情報の受渡しシステム。

【請求項９】　請求項１または２記載において、前記情報の種類によって分類される種別キーが前記共通キーに付加されていることを特徴とする情報の受渡しシステム。

【請求項１０】　請求項１または２記載において、前記共通キーの有効期限を示す期限キーが前記共通キーに付加されていることを特徴とする情報の受渡しシステム。

【請求項１１】　少なくとも情報を暗号化するための暗号論理手段と、暗号化のためのキーを格納するキー格納手段と、前記暗号論理手段を作動して情報の暗号化、復号化を行うセキュリティ処理手段とをそれぞれ有する第１の端末装置と第２の端末装置とを備え、

前記第１の端末装置において、情報の利用者間で共通する共通キーを生成し、情報利用者毎に個別に設定された個別キーで前記共通キーを暗号化して情報利用者毎の個別のワークキーを生成して、渡すオリジナルの情報を前記共通キーで暗号化して暗号化情報を生成する機能を有し、

前記第２の端末装置が固有の個別キーを有し、前記第１の端末装置からのワークキーを個別キーで復号化して共通キーを生成し、第１の端末装置からの暗号化情報を生成した共通キーで復号化してオリジナルの情報に相当する情報を生成する機能を有していることを特徴とする暗号処理装置。

【請求項１２】　少なくとも情報を暗号化するための暗号論理手段と、暗号化のためのキーを格納するキー格納手段と、前記暗号論理手段を作動して情報の暗号化、復号化を行うセキュリティ処理手段とをそれぞれ有する第１の端末装置と第２の端末装置とを備え、

前記第１の端末装置において、情報の利用者間で共通する共通キーを生成し、情報利用者毎に個別に設定された個別キーで前記共通キーを暗号化して情報利用者毎の個別のワークキーを生成して、第２の端末装置からの暗号化情報を前記共通キーで復号化してオリジナルの情報に相当する情報を生成する機能を有し、

前記第２の端末装置が固有の個別キーを有し、前記第１の端末装置からのワークキーを個別キーで復号化して共通キーを生成して、オリジナルの情報を暗号化する機能を有していることを特徴とする暗号処理装置。

【請求項１３】　少なくとも情報を暗号化するための暗号論理手段と、暗号化のためのキーを格納するキー格納

手段と、前記暗号論理手段を作動して情報の暗号化、復号化を行うセキュリティ処理手段とをそれぞれ有する第１の端末装置と第２の端末装置と第３の端末装置とを備え、

前記第１の端末装置において、情報の利用者間で共通する共通キーを生成し、情報利用者毎に個別に設定された個別キーで前記共通キーを暗号化して情報利用者毎の個別のワークキーを生成する機能を有し、

前記第２の端末装置が固有の個別キーを有し、前記第１の端末装置からのワークキーを個別キーで復号化して共通キーを生成して、オリジナルの情報を暗号化する機能を有し、

前記第３の端末装置が固有の個別キーを有し、前記第１の端末装置からのワークキーを個別キーで復号化して共通キーを生成して、第２の端末装置からの暗号化情報を前記共通キーで復号化してオリジナルの情報に相当する情報を生成する機能を有していることを特徴とする暗号処理装置。

【請求項１４】　請求項１１ないし１３記載のいずれかにおいて、前記端末装置が、キーならびに暗号化情報を送受信する通信手段を備えていることを特徴とする暗号処理装置。

【請求項１５】　請求項１１ないし１３記載のいずれかにおいて、前記端末装置が装置本体とその装置本体に対して着脱可能な携帯用のキー格納部材とから構成され、少なくともそのキー格納部材にキーを格納するキー格納手段が、前記装置本体にキー読取手段が、それぞれ設けられていることを特徴とする暗号処理装置。

【請求項１６】　請求項１５記載において、前記キー格納部材を装置本体に装着することにより、キー格納部材に格納されているキーを読み取るキー読取手段が装置本体に設けられていることを特徴とする暗号処理装置。

【請求項１７】　請求項１５記載において、前記キー格納部材にキーの読み取りアクセスを保護するキー照合手段が設けられていることを特徴とする暗号処理装置。

【請求項１８】　請求項１５記載において、前記キー格部材に装置本体が暗号処理手段と、キー読取手段と、セキュリティ処理手段と、通信手段を有し、前記着脱部材がキー格納手段と、キー照合手段と、通信手段を有していることを特徴とする暗号処理装置。

【請求項１９】　請求項１５記載において、１つの装置本体に対して２つ以上のキー格納部材を有し、各キー格納部材に格納されている個別キーの内容が異なっていることを特徴とする暗号処理装置。

【請求項２０】　請求項１１ないし１３記載のいずれかにおいて、前記端末装置が信号用アダプタに内蔵されていることを特徴とする暗号処理装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、機密保護を施した情報

の受渡しシステムならびにそれに用いる暗号処理装置に係り、さらに詳しくは、ソフトウェアの不正コピー防止が図れる機密性の高い情報の受渡しシステムとそれに用いる暗号処理装置に関するものである。

【０００２】

【従来の技術】従来、ソフトウェアのコピー防止については種々提案されているが、実際にはソフトウェアのセットアップ用ソフトでの使用回数のチェック、記憶装置の通常利用しないエリアのコードを該ソフトウェアの実行時に参照する等の簡単な方法が実用化されているに過ぎない。

【０００３】

【発明が解決しようとする課題】しかし、前述のようにソフトウェアのセットアップ回数のチェックやコードの参照などでは、機密の防止が不充分であった。

【０００４】特別の暗号処理装置を用いるものに、購入者自身がコピー防止希望時に自身のパスワードを該ソフトウェアに付加する方法もあったが、この方法は販売者又はレンタル会社が用いる方式には適用できず、複数種類のソフトに共通となるか、暗号処理装置をソフト毎に用意したり、差換えなければならないという不便さがあった。

【０００５】又、ネットワークを利用して送受信する情報の暗号化に関しては、パソコンやワークステーションにキーなどを格納して暗号化する方法があるが、これらの装置のキーを参照することは、第３者にとって比較的容易であり、機密防止の点では弱いものであった。

【０００６】今後、無線ＬＡＮなどの普及により、情報が無制限に近い領域に配布されるとなると、高機密な暗号化方式、つまり、専用の暗号処理装置が必須となる。

【０００７】さらに、放送分野のペイーＴＶ（有料放送）では、放送情報の暗号化（スクランブル）が行なわれている。この方法は、視聴者は見たい番組を放送局に予め連絡し、自分のＩＤの入ったカード等を受信用デコーダに挿入し、放送局側に申出のカードＩＤかデコーダ番号を照合し、合致していれば所定の解読キーで復号化する方法である。

【０００８】従って、放送情報の中に、申出のＩＤかデコーダ番号かの識別のための情報を含める必要がある。又、暗号化に用いるキーが、利用者毎の個別キーや番組（ないしは情報）毎の種別キーを含めて用いない為、これらを用いた暗号化キーの配布は必要ないが、固定的なキーによるので、不正解読の機会が多い。これを補完するためデコーダ内で、予め放送側と約束した一定のルールで、一定時間毎にキーを変化をさせる必要があった。

【０００９】本発明の目的は、前述したような、ソフト不正コピー防止が購入者に限定されたり、ネットワーク上の通信における機密の解読が容易であったり、放送においては申出者の識別情報を付加しなければならないなどの欠点を有効に解消し、機密性の高い情報の受渡しシ

ステムならびにそれに用いる暗号処理装置を提供するにある。

【００１０】

【課題を解決するための手段】前記目的を達成するため、第１の本発明は、少なくとも第１の端末装置と第２の端末装置との間で情報の受渡しを行う情報の受渡しシステムにおいて、次の処理工程を含んでいることを特徴とする。

【００１１】前記第１の端末装置で、情報の利用者間で共通する共通キーを生成し、その第１の端末装置において、情報利用者毎に個別に設定された個別キーで前記共通キーを暗号化して個別のワークキーを生成し、そのワークキーを前記第２の端末装置に渡し、第２の端末装置が有している個別キーを用いて、前述の渡されたワークキーを復号化して共通キーを生成し、渡す情報を前記共通キーで暗号化して暗号化情報を生成し、第１の端末装置または第２の端末装置から、他方の端末装置へ暗号化された情報を渡し、その渡された暗号化情報を共通キーを用いて元の情報に復号化する。

【００１２】前記目的を達成するため、第２の本発明は、少なくとも第１の端末装置と第２の端末装置と第３の端末装置の間で情報の受渡しを行う情報の受渡しシステムにおいて、次の処理工程を含んでいることを特徴とする。

【００１３】前記第１の端末装置で、情報の利用者間で共通する共通キーを生成し、その第１の端末装置において、情報利用者毎に個別に設定された個別キーで前記共通キーを暗号化して個別のワークキーを生成し、そのワークキーを前記第２の端末装置ならびに第３の端末装置にそれぞれ渡し、第２の端末装置ならびに第３の端末装置が有している個別キーを用いて、前述の渡されたワークキーを復号化して共通キーを生成し、渡す情報を前記共通キーで暗号化して暗号化情報を生成し、第１の端末装置、第２の端末装置、第３の端末装置の間で暗号化された情報を渡し、その受渡たされた暗号化情報を共通キーを用いて元の情報に復号化する。

【００１４】前記目的を達成するため、第３の本発明は、少なくとも情報を暗号化するための暗号論理手段と、暗号化のためのキーを格納するキー格納手段と、前記暗号論理手段を作動して情報の暗号化、復号化を行うセキュリティ処理手段とをそれぞれ有する第１の端末装置と第２の端末装置とを備えている。

【００１５】そして前記第１の端末装置において、情報の利用者間で共通する共通キーを生成し、情報利用者毎に個別に設定された個別キーで前記共通キーを暗号化して情報利用者毎の個別のワークキーを生成して、渡すオリジナルの情報を前記共通キーで暗号化して暗号化情報を生成する機能を有し、前記第２の端末装置が固有の個別キーを有し、前記第１の端末装置からのワークキーを個別キーで復号化して共通キーを生成し、第１の端末装置からの暗号化情報を生成した共通キーで復号化してオリジナルの情報に相当する情報を生成する機能を有していることを特徴とする。

【００１６】前記目的を達成するため、第４の本発明は、少なくとも情報を暗号化するための暗号論理手段と、暗号化のためのキーを格納するキー格納手段と、前記暗号論理手段を作動して情報の暗号化、復号化を行うセキュリティ処理手段とをそれぞれ有する第１の端末装置と第２の端末装置とを備えている。

【００１７】そして前記第１の端末装置において、情報の利用者間で共通する共通キーを生成し、情報利用者毎に個別に設定された個別キーで前記共通キーを暗号化して情報利用者毎の個別のワークキーを生成して、第２の端末装置からの暗号化情報を前記共通キーで復号化してオリジナルの情報に相当する情報を生成する機能を有し、前記第２の端末装置が固有の個別キーを有し、前記第１の端末装置からのワークキーを個別キーで復号化して共通キーを生成して、オリジナルの情報を暗号化する機能を有していることを特徴とする暗号処理装置。

【００１８】前記目的を達成するため、第５の本発明は、少なくとも情報を暗号化するための暗号論理手段と、暗号化のためのキーを格納するキー格納手段と、前記暗号論理手段を作動して情報の暗号化、復号化を行うセキュリティ処理手段とをそれぞれ有する第１の端末装置と第２の端末装置と第３の端末装置とを備えている。

【００１９】そして前記第１の端末装置において、情報の利用者間で共通する共通キーを生成し、情報利用者毎に個別に設定された個別キーで前記共通キーを暗号化して情報利用者毎の個別のワークキーを生成する機能を有し、前記第２の端末装置が固有の個別キーを有し、前記第１の端末装置からのワークキーを個別キーで復号化して共通キーを生成して、オリジナルの情報を暗号化する機能を有し、前記第３の端末装置が固有の個別キーを有し、前記第１の端末装置からのワークキーを個別キーで復号化して共通キーを生成して、第２の端末装置からの暗号化情報を前記共通キーで復号化してオリジナルの情報に相当する情報を生成する機能を有していることを特徴とする。

【００２０】

【作用】本発明は前述のような構成になっており、情報の暗号化は同一（共通）の値（内容）の共通キーＲを使用しているから、情報に対しては共通キーＲのみで一様に生産すればよいから処理が簡便である。

【００２１】また、情報の利用者ごとに異なる値（内容）のワークキー（Ｒ）Ｓｉを配布しているから、それの解読は非常に困難である。

【００２２】さらに情報の配布側と利用者側との間は、暗号化された情報（Ｉ）Ｒとワークキー（Ｒ）Ｓｉしか流れないので、機密は高度に保たれるなどの特長を有している。

【００２３】

【実施例】図１は、本発明の実施例に係る基本構成例を示すブロック図である。携帯できる暗号処理装置１（ＳＡＭ：Ｓｅｃｕｒｉｔｙ　Ａｃｃｅｓｓ　Ｍｏｄｕｌｅ）は、基本的には暗号論理手段３、キー格納手段５、セキュリティ処理手段７ならびに通信手段９から構成されている。

【００２４】前記暗号論理手段３は、情報ならびにキーを暗号化するための各種の暗号論理が格納されている。暗号論理手段３として、例えばＤＥＳ，ＲＳＡ，Ｍｕｌｔｉ，ＦＥＡＬ、０知識認証などがあるが、これらに限らず、暗号論理の全般のものが適用可能である。それの実施方法も、ＡＳＩＣで専用回路を組むことも、既存ワンチップマイコンを用いることも可能である。

【００２５】前記キー格納手段５には、後述するように共通キー、個別キー、ワークキー、種別キー、期限キーなどの各種キーが格納されるようになっている。

【００２６】このキー格納手段５には、電源非供給時も消去されないＥＥＰＲＯＭ、フラッシュメモリ、ＥＰＲＯＭなどが使用される。動作電源は、ＲＳ２３２Ｃの場合、パソコン本体から供給を受けることがてきる。ＪＥＩＤＡ４．１インタフェースでは、内部に電池を保有することになる。

【００２７】前記セキュリティ処理手段７は、キー格納手段５に格納されているキーの中から必要なキーを呼び出し、通信手段９を介して受け取られた情報を暗号論理手段３を用いて処理する機能を有している。

【００２８】なお、キー格納手段５から必要なキーを呼び出すとき、呼び出すためのアクセスチェックとして、パスワードチェックすることもあるし、暗号を用いた相互認証することもある。

【００２９】前記通信手段９は、外部との間で情報やキーなどの送受信を行なう機能を有している。この通信手段９は必ずしも１つであるとは限らず、例えばパソコンのＲＳ２３２Ｃに直付けのコンタクトと他方外部の装置、例えばモデムなどと透過的（トランスピアレント）につなぐための出口としてのＲＳ２３２Ｃのコンタクトの２つを持つこともある。ＪＥＩＤＡ４．１インタフェースでパソコンとつなぎ、一方で、出口としてＬＡＮの１０ＢＡＳＥ－Ｔのコンタクト、ないしはモデムやモデムＦＡＸを兼用の時は電話回線のスロットなどを持つこともある。

【００３０】図１は情報を供給する側の暗号処理装置（端末装置）Ｘと、その情報を受ける側の暗号処理装置（端末装置）Ｙとに分けて図示しており、ここでは情報を供給する側の暗号処理装置が１個で、情報を受ける側の暗号処理装置Ｙが２個の例を示しているが、実際には暗号処理装置Ｙの数は多数であることが多い。またこの例では、暗号処理装置１の構成が全て同じ例が示されている。

【００３１】前述のようにキー格納手段５には個別キーと共通キーが格納されており、図２はその個別キーと共通キーの関係をソフト不正コピー防止の用途を例にして示している図である。

【００３２】この例は、ソフトデータの情報１０を、第１の端末装置である暗号処理装置１｛ＳＡＭ（１）｝から第２の端末装置である暗号処理装置４｛ＳＡＭ（２）｝を介して伝送する例を示している。

【００３３】携帯暗号処理装置１｛ＳＡＭ（１）｝が、情報１０｛Ｉ（１）｝の暗号化を図るべく共通キーＲを生成する（同図のステップ　）。この生成は例えば図１の暗号論理手段３を用いて、乱数発生させれば容易に生成できる。ソフトデータの情報１０は、同図に示すように例えばフロッピーディスクなどの情報記録媒体に格納されており、その情報１０はリーダライターを介して読み出される（ステップ　）。

【００３４】そしてこの共通キーＲを用いて、前記情報１０｛Ｉ（１）｝を暗号化する（ステップ　）。この時の暗号化は、情報１０の全体を暗号化してもよいし、一部分暗号化してもよいし、また情報に付加する付加情報（暗号化結果やハッシュトータル、ないしはパスワード、暗号化パスワード、パスワードチェックロジック等）のみを暗号化してもよい。

【００３５】共通キーＲは、情報１０ごと（例えば：ソフトなら一太郎とか、ロータス１，２，３、などの種類ごと）に変えることが好ましい。暗号化された情報（Ｉ）Ｒは、オリジナルの情報Ｉ（１）とは区別し、暗号化情報（Ｉ）Ｒのみが暗号処理装置４｛ＳＡＭ（２）｝へ例えば通信手段などを使用して送られるか、製品に同梱されて配布され（ステップ　）、オリジナルの情報Ｉ（１）は配布されない。

【００３６】次に共通キーＲを個別キーＳｉで暗号化して、ワークキー（Ｒ）Ｓｉを生成する（ステップ　）。個別キーＳｉは、図１のキー格納手段５に予め格納されていると同時に、利用者の側にある携帯暗号装置４｛ＳＡＭ（２）｝にも予め付与されている。

【００３７】ＳＡＭ（１）１からＳＡＭ（２）４へワークキー（Ｒ）Ｓｉが、例えば通信手段９などを使用して送られるか、同梱されて渡される（ステップ　）。ＳＡＭ（２）４側では、予め格納、保有している利用者自身の個別キーＳｉでワークキー（Ｒ）Ｓｉを復号化して、共通キーＲを生成する（ステップ　）。　この共通キーＲで、さらに暗号化情報（Ｉ）Ｒを復号化して情報１０｛Ｉ（１）｝と同じソフトデータの情報１４｛Ｉ（２）｝を得て（ステップ　）、それをフロッピーディスクなどの情報記録媒体に格納することにより（ステップ　）、ソフトデータが不正にコピーされずに伝送される。ここでいう情報記録媒体は、例えばＦＤ、ＭＯ、ＣＤ－ＲＯＭ、テープ、カードなど各種の記録媒体が使用可能である。

【００３８】前述のように利用者ごとに異なる値（内容）のワークキー（Ｒ）Ｓｉを配布しているが（従ってこれを盗まれても、１人１人利用者毎に異なっているので、解読できない。）、暗号化は同一（共通）の値（内容）の共通キーＲを使用しているから、情報に対しては共通キーＲのみで一様に生産すればよい。配布側と利用者側との間は、暗号化された情報（Ｉ）Ｒとワークキー（Ｒ）Ｓｉしか流れないので、機密は高度に保たれている。

【００３９】ここでは説明を簡略化するため期限キーや種別キーの記述は省略したが、共通キーに期限キーや種別キーを加えて暗号化することもできる。すなわち、期限キーにより共通キーに有効期限を設け、その期限を経過した共通キーは使用できないシステムにすることができる。

【００４０】また、伝送されるべき情報を例えば技術的、用途的、内容的、地理的など適宜な種類に分類し、各種類に対応させて種別キーを設定し、情報ごとにアクセス権を分けることができる。

【００４１】前記図２では、情報の提供側と情報を受ける側が１対１の場合について説明したが、図３～８は情報を受ける側あるいは情報の提供側が複数ある場合を示している。

【００４２】図３に示されているように、情報の提供側である１つのＳＡＭ（１）に対して情報を受ける側に２つのＳＡＭ（２）－Ａ、ＳＡＭ（２）－Ｂが設置されている。

【００４３】そして前記ＳＡＭ（１）にはＳＡＭ（２）－Ａ用の個別キーＳｉ－ＡとＳＡＭ（２）－Ｂ用の個別キーＳｉ－Ｂが予め生成されて格納されているとともに、ＳＡＭ（２）－Ａには個別キーＳｉ－Ａが、ＳＡＭ（２）－Ｂには個別キーＳｉ－Ｂが、それぞれ予め付与、保有されており、個別キーＳｉ－Ａと個別キーＳｉ－Ｂは別の値（内容）を有する固有のものである。

【００４４】先ず、ＳＡＭ（１）において共通キーＲを生成する（ステップ　）。

【００４５】そして共通キーＲを前記個別キーＳｉ－ＡならびにＳｉ－Ｂで暗号化して、ＳＡＭ（２）－Ａ用のワークキー（Ｒ）Ｓｉ－Ａと、ＳＡＭ（２）－Ｂ用のワークキー（Ｒ）Ｓｉ－Ｂとを生成する（ステップ　）。このとき前述のように、共通キーＲに期限キーあるいは（ならびに）種別キーなど他のキーを付加して暗号化することもできる。

【００４６】生成したワークキー（Ｒ）Ｓｉ－ＡをＳＡＭ（２）－Ａに、ワークキー（Ｒ）Ｓｉ－ＢをＳＡＭ（２）－Ｂにそれぞれ個別に送る（ステップ　）。

【００４７】ＳＡＭ（２）－ＡならびにＳＡＭ（２）－Ｂでは、送られたワークキー（Ｒ）Ｓｉ－Ａ、（Ｒ）Ｓｉ－Ｂをそれぞれの個別キーＳｉ－ＡならびにＳｉ－Ｂを用いて復号化して共通キーＲを生成する（ステップ

）。以上のステップ　～　で、情報伝送のための準備が終了する。

【００４８】次にＳＡＭ（１）において、伝送すべきオリジナル情報Ｉ（１）を前記共通キーＲで暗号化して、暗号化情報（Ｉ）Ｒを生成する（ステップ　）。

【００４９】この暗号化情報（Ｉ）Ｒを、送付先のＳＡＭ（２）－Ａ、ＳＡＭ（２）－Ｂにそれぞれ送る（ステップ　）。

【００５０】ＳＡＭ（２）－ＡならびにＳＡＭ（２）－Ｂでは、送られた暗号化情報（Ｉ）Ｒを前記共通キーＲで復号化して、前記オリジナル情報Ｉ（１）に相当する情報Ｉ（２）を生成して（ステップ　）、情報の伝送を終了する。

【００５１】図４は、情報伝送の変形例を示す図である。この例で図３に示す処理と相違する点は、ＳＡＭ（１）でワークキー（Ｒ）Ｓｉと暗号化情報（Ｉ）Ｒを生成した後、これらを同時にＳＡＭ（２）－ＡならびにＳＡＭ（２）－Ｂに送っている点である。なお、これらの情報を送るときには、同一の伝送ルートで送ってもよいし、例えばネットワークとファックスなど別の伝送ルートで送ってもよい。

【００５２】図５は、情報伝送の他の変形例を示す図である。この例で図３に示す処理と相違する点は、ＳＡＭ（２）－ＡとＳＡＭ（２）－Ｂが予め個別キーＳｉ－Ａ、Ｓｉ－Ｂを保有しているのではなく、情報を伝送する前にＳＡＭ（１）で個別キーＳｉ－Ａ、Ｓｉ－ＢをＳＡＭ（２）－ＡとＳＡＭ（２）－Ｂにそれぞれ送付する点である。ＳＡＭ（１）での個別キーＳｉ－Ａ、Ｓｉ－Ｂの生成（更新、変更）は定期的であっても不定期的であってもよい。

【００５３】図６は、情報伝送のさらに他の変形例を示す図である。この例の場合、それぞれ個別キーＳｉ－Ａ、Ｓｉ－Ｂを保有しており、ＳＡＭ（１）で共通キーＲを生成（ステップ　）し、ワークキー（Ｒ）Ｓｉを生成（ステップ　）し、それをＳＡＭ（２）－ＡならびにＳＡＭ（２）－Ｂへ送付（ステップ　）して、ＳＡＭ（２）－ＡならびにＳＡＭ（２）－Ｂで共通キーＲを生成する（ステップ　）。

【００５４】次にＳＡＭ（２）－Ａ側が保有しているオリジナルの情報Ｉ（１）－ＡをＳＡＭ（２）－Ａで共通キーＲを使用して暗号化情報（Ｉ）Ｒ－Ａを生成し、それをＳＡＭ（１）に送る（ステップ　）。

【００５５】ＳＡＭ（１）ではこの暗号化情報（Ｉ）Ｒ－Ａを共通キーＲで復号化してＳＡＭ（２）－Ａ側の情報Ｉ（２）－Ａを生成する（ステップ　）。

【００５６】また、ＳＡＭ（２）－Ｂ側が保有しているオリジナルの情報Ｉ（１）－ＢをＳＡＭ（２）－Ｂで共通キーＲを使用して暗号化情報（Ｉ）Ｒ－Ｂを生成し、それをＳＡＭ（１）に送る（ステップ　）。

【００５７】ＳＡＭ（１）ではこの暗号化情報（Ｉ）Ｒ

－Ｂを共通キーＲで復号化してＳＡＭ（２）－Ｂ側の情報Ｉ（２）－Ｂを生成する（ステップ　）。

【００５８】図７は、情報伝送のさらに他の変形例を示す図である。この例で前記図６の処理と相違する点は、ステップ　において暗号化情報（Ｉ）Ｒ－ＡをＳＡＭ（１）とＳＡＭ（２）－Ｂへ送り、ＳＡＭ（１）ならびにＳＡＭ（２）－Ｂでこの暗号化情報（Ｉ）Ｒ－Ａを共通キーＲで復号化してＳＡＭ（２）－Ａ側の情報Ｉ（２）－Ａを生成する（ステップ　）点である。

【００５９】図８は、ネットワーク上で本発明の暗号処理装置を使用した場合の構成例を示す図である。図中の３０Ａは情報を提供しようとするセキュリティサーバ側のパソコンで、暗号処理装置１が装着されている。３０Ｂはクライアント－１側のパソコンで暗号処理装置４ａが装着され、３０Ｃはクライアント－２側のパソコンで暗号処理装置４ｂが装着されている。これらパソコン３０Ａ，３０Ｂ，３０Ｃは、ＬＡＮや無線ＬＡＮなどのネットワークシステム２２によって相互に接続されている。

【００６０】同図に示すように暗号処理装置１において共通キーＲを生成（ステップ　）し、個別キーＳｉを用いてワークキー（Ｒ）Ｓｉを生成（ステップ　）し、パソコン３０Ａからネットワークシステム２２を介してワークキー（Ｒ）Ｓｉ－Ａを暗号処理装置４ａに、ワークキー（Ｒ）Ｓｉ－Ｂを暗号処理装置４ｂに、それぞれ送信する（ステップ　）。

【００６１】そして暗号処理装置４ａではワークキー（Ｒ）Ｓｉ－Ａを復号化して共通キーＲを生成し、暗号処理装置４ｂではワークキー（Ｒ）Ｓｉ－Ｂを復号化して共通キーＲを生成する（ステップ　）。

【００６２】フロッピーディスクなどの情報記録媒体２１をパソコン３０Ｂに装着して、情報記録媒体２１内のオリジナル情報Ｉを読出し、それを共通キーＲで暗号化して暗号化情報（Ｉ）Ｒを得る（ステップ　）。

【００６３】この暗号化情報（Ｉ）Ｒをネットワークシステム２２を介してパソコン３０Ｃに送り（ステップ　）、暗号処理装置４ｂにおいて暗号化情報（Ｉ）Ｒを共通キーＲで復号化してオリジナル情報Ｉに相当する情報を得る（ステップ　）ようなシステムになつている。

【００６４】図９は図８で説明したパソコン３０Ｂの側面図、図１０はそのパソコン３０Ｂに接続された暗号処理装置４ａの処理動作を説明するためのフローチャートである。

【００６５】図９に示されているように、パソコン３０Ｂの後部にある通信用スロットにアダプタ２０が接続され、それに暗号処理装置４ａが内蔵されて、ネットワークシステム２２用のケーブル２３が付設されている。

【００６６】次に暗号処理装置４ａの処理動作について図１０とともに説明する。まず、ステップ（Ｓ）１においてパソコン３０Ｂ側から暗号処理装置４ａにデータ伝送の命令信号が入力される。Ｓ２では、その命令信号がアダプタ２０の所定のピンＮＯ．に送付されたかどうかのチェツクがなされる。例えばアダプタ２０に２５本のピンがあり、そのうちのピンＮＯ．１～６がセキュリティ処理に使用されるように設定されている。

【００６７】命令信号が所定のピンＮＯ．に送付されたことを確認すると、Ｓ３で復号化命令が出されたかどうか判断され、復号化命令が出されておれば次のＳ４に、そうでなければ後段のＳ６に進む。

【００６８】Ｓ４で暗号処理装置４ａに予め格納されている個別キーＳｉが呼び出され、パソコン３０Ａから送付されたワークキー（Ｒ）Ｓｉを復号化して共通キーＲを生成し、Ｓ５でその共通キーＲを暗号処理装置４ａに格納して、終了レスポンスをパソコン３０Ｂに返信する。

【００６９】次に共通キーＲの要求があったかどうか判断され、あると判断されると次のＳ７に、ないと判断されると後段のＳ９に進む。Ｓ７で共通キーＲをレスポンスし、Ｓ８において共通キーＲを用いてオリジナル情報Ｉを暗号化して、その暗号化情報（Ｉ）Ｒを受領者であるパソコン３０Ｃにネットワークシステムを介して伝送する。

【００７０】そしてＳ９で期限チェツクなど暗号処理装置４ａに関する命令等を全て処理した後、その暗号処理装置４ａに対して暗号処理の機能をもたないで単にケーブルとして見做すスルー処理を行なう。

【００７１】次に、実際の種別キーを存在させた場合のソフト販売またはレンタル時の運用について述べる。

【００７２】図１１は、図１に示したキー格納手段５をＳＡＭ１から分離させた場合を示しており、分離させることにより暗号処理装置ＳＡＭ１がＳＡＭ１ａとＳＡＭ１ｂに分かれる。

【００７３】そして暗号処理装置ＳＡＭ１ａは同図に示すように、暗号論理手段３と、キー読取手段６と、セキュリティ処理手段７ａと、通信手段９ａとから主に構成されている。

【００７４】一方、コンパクトな携帯用の暗号処理装置ＳＡＭ１ｂは、キー格納手段５と、キー照合手段８と、通信手段９ｂとから主に構成されている。このＳＡＭ１ｂは、例えばシリアルメモリを持ったカードやペンシル型棒やコインなどであり、シリアルメモリはキー照合手段８によってパスワードチェックがＯＫなら中のキー情報を呼び出せる構成になっている。メモリはＥＥＰＲＯＭ、フラッシュメモリ、ＥＰＲＯＭなどから構成されており、消去されず、電源も不要で、低コストの携帯キーとなる。

【００７５】これに個別キーＳｉや期限キー、種別キーなど必要な各種キーを格納して、情報の入った記録媒体（ＦＤやその他）と共に梱包され、販売時又はレンタル時に利用者に渡される。シリアルメモリに限らず、ＩＣ

カード、ＣＰＵ付きペンやコイン、磁気カードなど各種のものが使用可能である。

【００７６】利用者は、自分の許にあるＳＡＭ１ａに、このＳＡＭ１ｂをセットしてキーの呼出しを行なう。もし、情報が複数の場合には各々にＳＡＭ１ｂが存在するので、ＳＡＭ１ａはこれらの複数のＳＡＭ１ｂをＳＡＭ１ａ内に一度だけ格納すればよい。このようにＳＡＭ１ｂを分けて、携帯可能に、又は暗号化情報（Ｉ）Ｒと同梱させることにより、高機密でコピーが不可能な状態になる。

【００７７】ネットワーク上で情報のメールを高機密に行う場合、ワークステーションを一人で使用するのならＳＡＭ１ｂは無くても図１のＳＡＭ１で済み、ワークステーション１台を数人で使う時は、各自のＳＡＭ１ｂを使用時にＳＡＭ１ａにセットすればよい。

【００７８】ネットワークの場合、種別キーは無いが、期限キーはあってもよい。暗号化情報（Ｉ）Ｒは、ネットワークを介して伝送される。受信者は、予めセキュリティサーバから送られて来ているワークキー（Ｒ）Ｓｉを復号化して、共通キーＲを得て、この共通キーＲで暗号化情報（Ｉ）Ｒを復号化して情報を読むことになる。

【００７９】個別キーＳｉや期限キー、暗号関数がワークステーションのハードディスクやメモリに格納されていると、盗聴されたり、ファイルがコピーされたりして、キーや暗号関数が盗まれる可能性が高い。しかし、本発明のＳＡＭ１を用いれば、これらは特別のハードの中にパスワード付きで内蔵され、呼出されるものはその一部の情報でそれしか外に出ないで、又、それを保有していないと動作しないので、機密性が非常に高い。

【００８０】放送用のペイーＴＶに用いる場合でも、ネットワークとほぼ同様で、各視聴者に予めワークキー（Ｒ）Ｓｉを配布し、個別キーＳｉを内蔵したＩＣカード等にてワークキー（Ｒ）Ｓｉを復号化して、共通キーＲを得る。その共通キーＲで、暗号化情報（Ｉ）Ｒをオリジナル情報Ｉと同じ状態に復号化する。

【００８１】図１２～１５は、各実施例に係る携帯暗号処理装置の外観図である。図１２は、パソコンやＷＳ３０の通信スロット（ＲＳ２３２Ｃスロット）などの入出力装置に、暗号処理装置ＳＡＭ１をアダプタの型で接続した場合を示している。

【００８２】図中の２０はアダプタで前記ＳＡＭ１が組み込まれており、２４は外向きのＲＳ２３２Ｃスロット、又はＬＡＮインターフェース、又は電話接続コンタクト、２５はパソコンやＷＳ３０のＲＳ２３２Ｃスロットなどの入出力装置、３０はパソコンのワークステーションである。なお、暗号処理装置ＳＡＭ１の電源はパソコン３０側から供給されるようになっている。

【００８３】この実施例では前記アダプタ２０を入出力装置２５に接続することにより、本来のアダプタの機能の他に暗号処理機能が発揮でき、それも、利用者にとっては、従来通りの入出力機能のみ意識で、暗号処理装置の機能は意識することなく、いわゆる透過的（トランスピアレント）に両機能が実現できるという特長を有している。

【００８４】また、前記アダプタ２０はＬＡＮ制御機能を内蔵し、外向きのインタフェース２４として例えばＬＡＮ用の１０－Ｂａｓｅ－Ｔ、１０－Ｂａｓｅ－５、１０－Ｂａｓｅ－１０などの入出力ポート、ＲＳ２３２Ｃなどのシリアルポート、ＳＣＳＩ、ＩＤＥなどの既存のインタフェースポート、汎用の拡張ボードや専用の内蔵ボード、ＳＩＭＭなどを利用することもできる。アダプタ２０がファックスやモデムを兼用するときは出力口は電話接続用コンタクトとなり、無線ＬＡＮ対応の受発信機でもよい。

【００８５】図１３は、暗号処理装置ＳＡＭ１がＳＡＭ１ａとＳＡＭ１ｂの２つに分かれ、ＳＡＭ１ｂ（ＳＡＭ１ｂ－１，ＳＡＭ１ｂ－２，……ＳＡＭ１ｂ－ｎ）が利用者ごとに異なった場合の外観図である。

【００８６】ＳＡＭ１ａはアダプタ本体２０ａに内蔵され、ＳＡＭ１ｂ（ＳＡＭ１ｂ－１，ＳＡＭ１ｂ－２，……ＳＡＭ１ｂ－ｎ）は例えばペン型の着脱部材２０ｂに内蔵され、この着脱部材２０ｂはアダプタ本体２０ａに対して着脱可能になっている。この例では着脱部材２０ｂは接続式のインタフェースを有しており、抜き出した時は胸のポケットにペン同様に収納できる。

【００８７】また、アダプタ本体２０ａと着脱部材２０ｂにそれぞれ信号送受信用ならびに給電用のコイルを設け、着脱部材２０ｂをアダプタ本体２０ａに装着するかあるいは近づけることにより、両コイル間の磁気的結合を利用してＳＡＭ１ａとＳＡＭ１ｂの間で信号の送受信と電力の供給を行うこともできる。

【００８８】図１４は、ＳＡＭ１ａとＳＡＭ１ｂがともにカード状になってに分かれる暗号処理装置の外観図である。

【００８９】ＳＡＭ１ａはＩＣカードなどからなるカード本体４０に内蔵され、このカード本体４０に対して着脱可能なサブカード４１にＳＡＭ１ｂ（携帯キー格納装置）が内蔵されされている。

【００９０】カード本体４０の上面側にはサブカード４１が装着される凹部４２が形成され、その凹部４２内にはサブカード４１との接続を図るための接点バネ４３が設けられ、一方、サブカード４１の下面には接点バネ４３と接触する接点４４が設置されている。

【００９１】カード本体４０の前部には、ＬＡＮインターフェースやモデム、フアックスモデムのインターフェースなどからなる外向きインターフェース４５が設けられている。また、カード本体４０の後部には、ＪＥＩＤＡ４，１インターフェース４６が設けられている。

【００９２】この例では外部から機器の筐体を開ける作業をすることなく接続可能なＩＣメモリカードの例を示

したが、これに限らずパソコンの筐体を開けてセットする、例えば汎用拡張ボードや機器ごとの専用内蔵ボードでも同様に実現できる。これらの場合は、パソコンの立上げ時のＢｏｏｔセクタのコントロールまで可能なので、セキュリティ処理の実現がかなり容易になる。

【００９３】個人別のキー格納媒体のリーダライタの実装やＬＡＮ、モジュラーシックの出口の実装も該ボードで可能である。

【００９４】図１５は図１４の変形例で、図１４のサブカード４１の代わりに例えばペン型などの着脱部材４７が用いられ、それにＳＡＭ１ｂ（携帯キー格納装置）が内蔵されされている。そしてこの着脱部材４７が、カード本体４０に対して着脱可能に装着されている。

【００９５】本発明にかかる各種情報は、例えばフロッピーディスク、リードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－Ｉ、ＭＤ、メモリカード、コンピュータテープ、ＶＴＲテープ、カセットテープなどの情報記録媒体に格納されている。

【００９６】本発明の暗号処理装置の構成要素の１つ以上が、ＩＣメモリカードにて実現され、ＪＥＩＤＡ４，１などの標準インタフェースにて実現できる。またそのＩＣメモリカードが、前記キー格納部材の入出力装置となっており、ＪＥＩＤＡ４，１のインタフェースにＩＣメモリカードを挿入し、さらに、該ＩＣメモリカードにキー格納部材を接続して、一連の暗号処理を行うことができる。

【００９７】また前記ＩＣメモリカードが、通信用のモデム（変復調装置）、ファクシミリ送受信機能、無線通信機能、ローカルエリアネットワークインタフェース機能、などのいづれか１つか、複数の機能を実装し、暗号処理機能のみならず他の機能も発揮できて、該ＩＣメモリカードには、ＪＥＩＤＡ４，１，携帯キー格納装置の入出力インタフェースなどの他にモデム、ＦＡＸ、無線通信、ＬＡＮなどの入出力ポートをも具備することができる。

【００９８】前記携帯用のキー格納部材が、中央処理装置ＣＰＵを用いたマンチップマイコンによるもの、シリアルメモリによるもの、ＡＳＩＣ論理機構によるもの、磁気媒体によるもの、光学的コードの読書によるもの、電磁波によるもの、ラジオ周波数等の電波によるものなどの中の１つ又は、複数を用いて実現することも可能である。

【００９９】またＩＣメモリカードの代わりに、ＲＳ２３２Ｃのシリアルポートにケーブルレスにアタッチしたアダプタに本発明の暗号処理装置を内蔵し、該アダプタがパソコンと直接接続するポートの他に外部と接続するポートを有し、常時接続状態にすることもできる。

【０１００】本発明の暗号処理機能のうち、暗号処理装置が接続されているパソコン、ワークステーション、インテリジェント電話などの本体の側で、情報の暗号化や

復号化を行ない、携帯暗号処理装置で、キーの暗号化、復号化およびキーの格納、生成、照合など行なうように機能分担させることも可能である。

【０１０１】本発明に係る情報が、ネットワーク、パソコン通信、ＢＳやＣＳなどの有料無料の衛星放送、地上波やケーブルＴＶ、無線ネットワーク、電話網、無線電話網、アマチュア無線通信、などで送受信する情報、プログラム、データ、音声画像、などであり、送受の両方で、暗号化と復号化を行なうことによって、高機密に情報の受渡しや課金の処理を行なうことも可能である。

【０１０２】本発明による情報の暗号化、復号化は単に全ての情報の暗号化、復号化を指すのでなく、一部の情報を対象にするか、情報に付加するキーチェックモジュールを付加するか、情報自体をそのままにしてこれを暗号化したハッシュトータル値を付加するか、デジタル署名（認証コード）を行なうかなどのいづれか、または複数を行なうようにしてもよい。

【０１０３】また情報にはソフトウェアプログラムも含まれ、これらの情報を格納した記録媒体を販売又はレンタルする際、前記キー格納部材を同梱して配布し、そのキー格納部材に格納されているキーによって情報の暗号化処理がなされ、キー格納部材が情報の利用には不可欠のようにすることにより、ソフトウェアを含む情報の不正コピーを防止することができる。

【０１０４】さらに情報がコンピュータネットワークなどによって送信されて販売又はレンタルされる場合には、該情報を暗号化した際のキー、ないしは該キーを暗号化した暗号化キーを格納したキー格納部材を別送し、これを用いて、受信は情報を復号化し、利用できるようにする。

【０１０５】

【発明の効果】本発明は前述のような構成になっており、情報の暗号化は同一（共通）の値（内容）の共通キーＲを使用しているから、情報に対しては共通キーＲのみで一様に生産すればよいから処理が簡便である。

【０１０６】また、情報の利用者ごとに異なる値（内容）のワークキー（Ｒ）Ｓｉを配布しているから、それの解読は非常に困難である。

【０１０７】さらに情報の配布側と利用者側との間は、暗号化された情報（Ｉ）Ｒとワークキー（Ｒ）Ｓｉしか流れないので、機密は高度に保たれるなどの特長を有している。

【図面の簡単な説明】

【図１】本発明の実施例に係る情報の受渡しシステムを説明するための構成例を示すブロック図である。

【図２】その情報の受渡しシステムの流れを説明するための図である。

【図３】その情報の受渡しシステムの他の流れを説明するための図である。

【図４】その情報の受渡しシステムの他の流れを説明す

るための図である。

【図５】その情報の受渡しシステムの他の流れを説明するための図である。

【図６】その情報の受渡しシステムの他の流れを説明するための図である。

【図７】その情報の受渡しシステムの他の流れを説明するための図である。

【図８】その情報の受渡しシステムの他の流れを説明するための図である。

【図９】パソコンに暗号処理装置を接続した状態を示す側面図である。

【図１０】その暗号処理装置の動作を説明するためのフローチャートである。

【図１１】暗号処理装置の変形例を示すブロック図である。

【図１２】暗号処理装置を内蔵したアダプタの斜視図である。

【図１３】暗号処理装置を内蔵した他のアダプタの斜視図である。

【図１４】暗号処理装置の変形例を説明するための図である。

【図１５】暗号処理装置のさらに他の変形例を説明するための図である。

【符号の説明】

１　暗号処理装置

３　暗号論理手段

４　暗号処理装置

５　キー格納手段

７　セキュリティ処理手段

８　キー照合手段

９　通信手段

１０　情報Ｉ（１）

１４　情報Ｉ（２）

２０　アダプタ

２０ｂ　着脱部材

２１　情報記録媒体

２２　ネットワークシステム

２４　スロット

２５　入出力装置

３０　パソコン

４０　カード本体

４１　サブカード

４５、４６　インターフェース

４７　着脱部材

Ｒ　共通キー

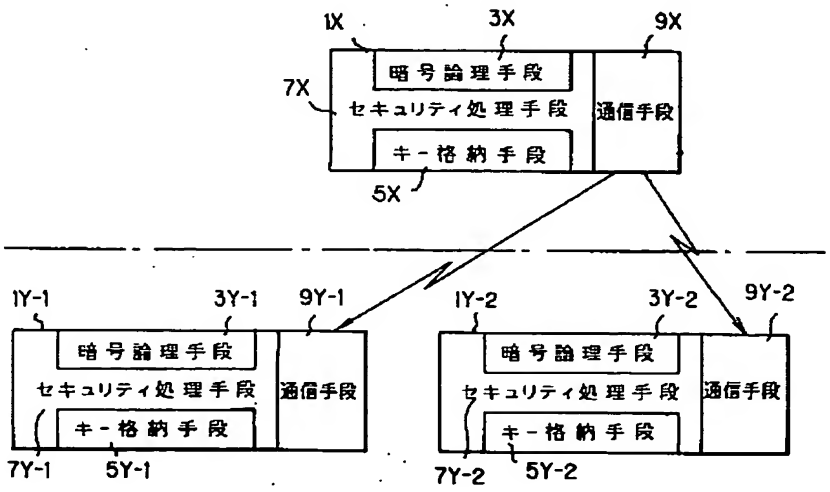
Ｓｉ　個別キー

（Ｒ）Ｓｉ　ワークキー

Ｉ（１）　オリジナル情報

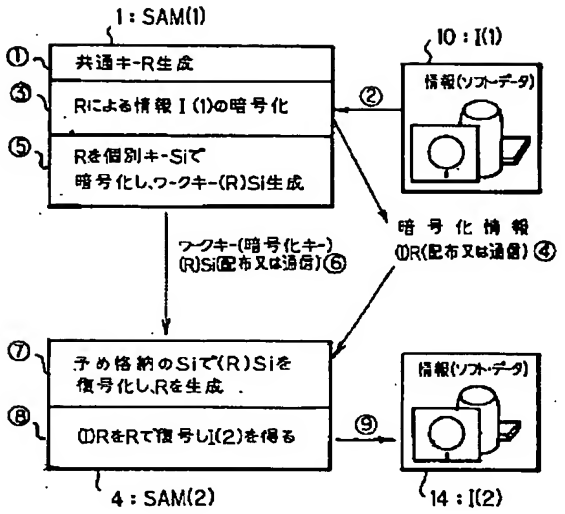
（Ｉ）Ｒ　暗号化情報

【図１】



【図２】

【図２】



【図３】

【図３】

SAM(1)	SAM(2)-A	SAM(2)-B
個別キ-Si-A、Si-Bを生成、保有。 ① 共通キ-Rを生成。 ② 共通キ-Rを個別キ-Si-A、Si-Bで暗号化して、ワークキ-(R)Si-A、(R)Si-Bを生成。 ③ ワークキ-(R)Si-AをSAM(2)-Aに、(R)Si-BをSAM(2)-Bにそれぞれ送る。 ⑤ オリジナル情報Ⅰ(1)を共通キ-Rで暗号化して暗号化情報(1)Rを生成。 ⑥ 暗号化情報(1)RをSAM(2)-A、SAM(2)-Bに、それぞれ送る。	個別キ-Si-Aを付与、保有。 ④ ワークキ-(R)Si-Aを個別キ-Si-Aで復号化して、共通キ-Rを生成。 ⑦ 暗号化情報(1)Rを共通キ-Rで復号化して、情報Ⅰ(2)を生成。	個別キ-Si-Bを付与、保有。 ④ ワークキ-(R)Si-Bを個別キ-Si-Bで復号化して、共通キ-Rを生成。 ⑦ 暗号化情報(1)Rを共通キ-Rで復号化して、情報Ⅰ(2)を生成。

【図４】

【図４】

SAM(1)	SAM(2)-A	SAM(2)-B
個別キ-Si-A、Si-Bを生成、保有。 ① 共通キ-を生成。 ② 共通キ-を個別キ-Si-A、Si-Bで暗号化して、ワークキ-(R)Si-A、(R)Si-Bを生成。 ③ オリジナル情報Ⅰ(1)を共通キ-Rで暗号化して、暗号化情報(1)Rを生成。 ④ ワークキ-(R)Si-A、(R)Si-Bと暗号化情報(1)Rを、SAM(2)-A、SAM(2)-Bに、それぞれ送る。	個別キ-Si-Aを付与、保有。 ⑤ ワークキ-(R)Si-Aを個別キ-Si-Aで復号化して、共通キ-Rを生成。 ⑧ 暗号化情報(1)Rを共通キ-Rで復号化して、情報Ⅰ(2)を生成。	個別キ-Si-Bを付与、保有。 ⑤ ワークキ-(R)Si-Bを個別キ-Si-Bで復号化して、共通キ-Rを生成。 ⑥ 暗号化情報(1)Rを共通キ-Rで復号化して、情報Ⅰ(2)を生成。

【図７】

【図７】

SAM(1)	SAM(2)-A	SAM(2)-B
個別キ-Si-A、Si-Bを生成、保有。 ① 共通キ-を生成。 ② 共通キ-を個別キ-Si-A、Si-Bで、暗号化して、ワークキ-(R)Si-A、(R)Si-Bを生成。 ③ ワークキ-(R)Si-A、(R)Si-BをSAM(2)-A、SAM(2)-Bへ、それぞれ送る。 ⑥ 暗号化情報(Ⅰ)R-Aを共通キ-Rで復号化して、情報Ⅰ(2)-Aを生成。	個別キ-Si-Aを付与、保有。 ④ ワークキ-(R)Si-Aを個別キ-Si-Aで復号化して、共通キ-Rを生成。 ⑤ オリジナル情報Ⅰ(1)-Aを共通キ-Rで暗号化して、暗号化情報(Ⅰ)R-AをSAM(1)とSAM(2)-Bへ送る。	個別キ-Si-Bを付与、保有。 ④ ワークキ-(R)Si-Bを個別キ-Si-Bで復号化して、共通キ-Rを生成。 ⑥ 暗号化情報(Ⅰ)R-Aを共通キ-Rで復号化して、情報Ⅰ(2)-Aを生成。

【図５】

【図５】

SAM(1)	SAM(2)-A	SAM(2)-B
①共通キ-Rを生成。 ②SAM(2)-A用、SAM(2)-B用の個別キ-Si-A、Si-Bを生成。 ③個別キ-Si-A、Si-BをSAM(2)-A、SAM(2)-Bへ、それぞれ送る。	④個別キ-Si-Aを格納。	④個別キ-Si-Bを格納。
⑤共通キ-Rを個別キ-Si-A、Si-Bで暗号化して、ワークキ-(R)Si-A、(R)Si-Bを生成。 ⑥ワークキ-(R)Si-A、(R)Si-BをSAM(2)-A、SAM(2)-Bへ、それぞれ送る。	⑦ワークキ-(R)Si-Aを個別キ-Si-Aで復号化して、共通キ-Rを生成。	⑦ワークキ-(R)Si-Bを個別キ-Si-Bで復号化して、共通キ-Rを生成。
⑧オリジナル情報I(1)を共通キ-Rで暗号化して、暗号化情報(I)Rを生成して、SAM(2)-A、SAM(2)-Bへ、それぞれ送る。	⑨暗号化情報(I)Rを共通キ-Rで復号化して、情報I(2)を生成。	⑨暗号化情報(I)Rを共通キ-Rで復号化して、情報I(2)を生成。

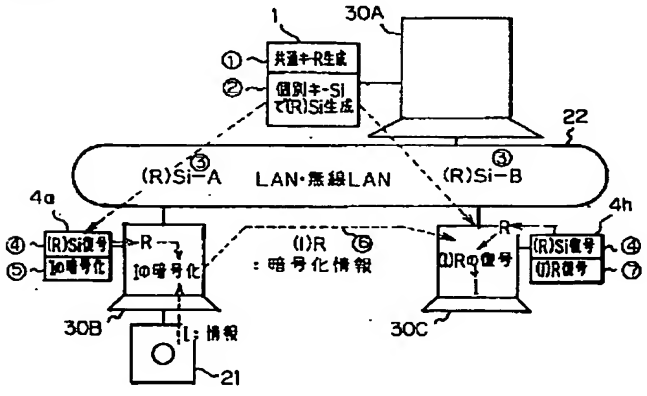
【図６】

【図６】

SAM(1)	SAM(2)-A	SAM(2)-B
個別キ-Si-A、Si-Bを生成、保有。 ①共通キ-を生成。 ②共通キ-を個別キ-Si-A、Si-Bで暗号化して、ワークキ-(R)Si-A、(R)Si-Bを生成。 ③ワークキ-(R)Si-A、(R)Si-BをSAM(2)-A、SAM(2)-Bへ、それぞれ送る。	個別キ-Si-Aを付与、保有。	個別キ-Si-Bを付与、保有。
	④ワークキ-(R)Si-Aを個別キ-Si-Aで復号化して、共通キ-Rを生成。 ⑤オリジナル情報I(1)-Aを共通キ-Rで暗号化して、暗号化情報(I)R-AをSAM(1)へ送る。	④ワークキ-(R)Si-Bを個別キ-Si-Bで復号化して、共通キ-Rを生成。
⑥暗号化情報(I)R-Aを共通キ-Rで復号化して、情報I(2)-Aを生成。		⑦オリジナル情報I(1)-Bを共通キ-Rで暗号化して、暗号化情報(I)R-BをSAM(1)へ送る。
⑧暗号化情報(I)R-Bを共通キ-Rで復号化して、情報I(2)-Bを生成。		

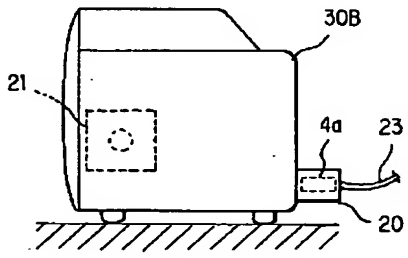
【図８】

【図８】



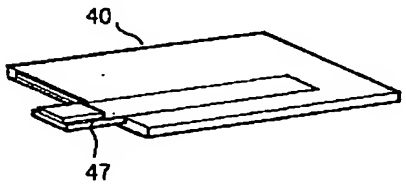
【図９】

【図９】



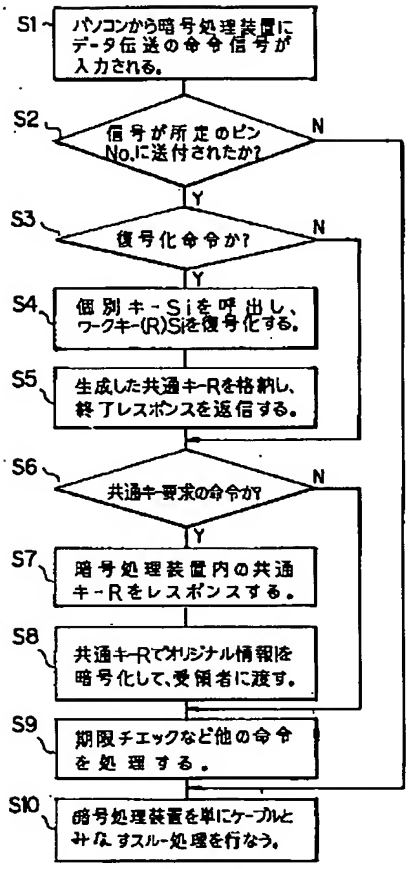
【図１５】

【図15】



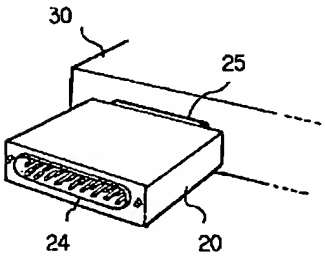
【図１０】

【図10】



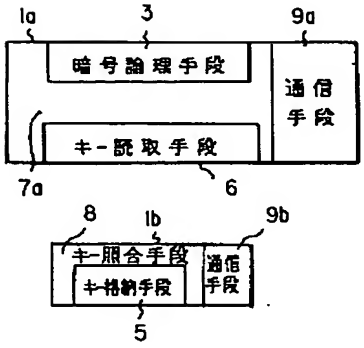
【図１２】

【図12】



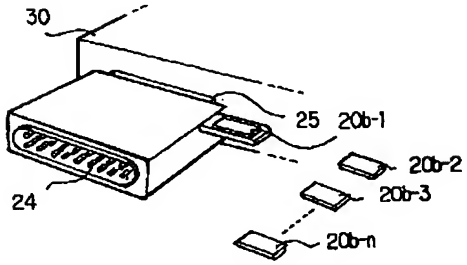
【図１１】

【図11】



【図１３】

【図13】



【図１４】

【図14】